UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/050,274	01/16/2002	Yoon Seok Yang	0465-2091PUS1	7037

2292 7590 06/16/2009

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
BROWN, CHRISTOPHER J	

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
06/16/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mailroom@bskb.com

Office Action Summary	Application No.	Applicant(s)	
	10/050,274	YANG, YOON SEOK	
	Examiner	Art Unit	
	CHRISTOPHER J. BROWN	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 May 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,9-13,18,21-23 and 25-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,9-13,18,21-23 and 25-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicants arguments filed 11/17/08 have been considered but are not persuasive.

Applicants have removed limitations which were previously indicated to be allowable, and argue that neither Wasilewski or Daemen teach a "start signal" when a new round key is needed.

The examiner argues that it is first inherent that the encryption as taught by Wasilewski and Daemen must get a start signal, because the key is needed for encryption, and both references teach encryption. Thus a signal must be sent to start encryption and request a key. Additionally, Daemen teaches that a cipher key is sent upon which the round keys are derived.on page 14, 4.3. Thus a cipher key input into the key schedule may be interpreted as this start key signal.

Applicants argue that the 35 USC 101 rejection is statutory, but the examiner disagrees. The word "apparatus" does not indicate sufficient hardware to make the subject matter patentable. As was discussed in the interview with the applicant, the specification indicates that the apparatus may be software or hardware.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

The claimed invention is directed to non-statutory subject matter. Claims 1, 10, and 22, and 25 are rejected under USC 101. Claims 1, 10, and 22 could be interpreted as pure software. Under *In re Bilski* subject matter must be tied to a specific machine or transform one substance to another. According to the specification the claimed block cipher may be a software program. Appropriate correction is required.

Claims 25-27 all claim a signal "start key signal", "data key valid" signal. Propagating signals are not patentable subject matter. Claims must incorporate a storage medium, a processor, or some sort of functional hardware that is supported by the instant specification such as the stated logic gates that make up the units as stated in the specification in paragraph [0049].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 5, 9-11, and 18, 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski US 5,420,866 in view of Daemen ("AES Proposal: Rijndael," March 1999),

As per claims 1, 10, and 22, Wasilewski teaches a control unit receiving a data stream of byte units where the data stream is an MPEG data stream (encoder) (Col 8 lines 52-60, Col 9 lines 58). Wasilewski does not explicitly teach converting data into block data for encryption. Wasilewski teaches encrypting the data with the DES protocol (Col 9 lines 8-12),

Daemen teaches encrypting the data with the AES protocol using blocks (page 8, "4 specification") Thus the MPEG stream must be converted into blocks to be encrypted. Wasilewski teaches outputting encrypted stream data, thus the blocks are converted from blocks back into bytes (Col 9 lines 30-36). Daemen teaches that the key may be of variable size 128, 192, or 256 bits (page 8 "4 specification"). Daemen teaches that a cipher key (start key signal) is sent upon which the round keys are derived (4.3). Daemen teaches a key schedule unit carrying out a key schedule for every round. Daemen teaches encrypting and decrypting data blocks. Daemen teaches that the key register has a capacity amounting to (size of inputted block) * (size of one round) (Daemen 4.3.2)

It would be obvious one of ordinary skill in the art to use the apparatus of Wasilewski with the protocol of Daemen to provide an encryption scheme that is efficient for use with low-end microprocessors.

As per claim 2, Wasilewski teaches a control unit receiving a data stream of byte units where the data stream is an MPEG data stream (encoder) (Col 8 lines 52-60, Col 9 lines 58). Wasilewski does not explicitly teach converting data into block data for encryption. Wasilewski teaches encrypting the data with the DES protocol (Col 9 lines 8-12), Daemen teaches that AES may use a predetermined block size of 128 bits, 192 or 256 bits. Thus Wasilewski teaches that the MPEG stream must be converted into blocks to be encrypted. Wasilewski teaches outputting encrypted stream data, thus the blocks are converted from blocks back into bytes (Col 9 lines 30-36).

As per claim 9, 21 Wasilewski teaches encrypting the data with the DES protocol. (Col 9 lines 8-12). Daemen teaches the key schedule may generate the key required for the block round in each round (page 17 5.1, key is updated between rounds).

As per claims 11, and 23 Wasilewski teaches the first format is a byte unit (MPEG stream (Col 9 lines 8-15). Daemen teaches a second format is a block unit (AES block), (page 8, Specification).

As per claims 5, and 18, 21 Wasilewski does not specify the inputted key value and size. Daemen teaches a key size of 128 bits (page 14 4.3) and an expansion algorithm for the Rijndael block cipher wherein the key expansion unit expands the inputted key value into a size amounting to {block size * (count of rounds + 1)} (page 14, section 4.3.1) for the

purpose of proposing a new encryption standard that is, among other things, efficient for use with 8-bit microprocessors (page 28, section 7.5). Daemen further teach that the key register has a capacity amounting to {(size of an inputted block) * (size of one round)} (Daemen, section 4.3.2). It is inherent that the key is stored in a key register.

Claims 3, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski US 5,420,866 in view of Daemen ("AES Proposal: Rijndael," March 1999)in view of Mroczkowski ("Implementation of the block cipher Rijndael using Altera FPGA," May 2000)

As per claim 12, Wasilewski teaches a control unit receiving a data stream of byte units where the data stream is an MPEG data stream (encoder) (Col 8 lines 52-60, Col 9 lines 58). Wasilewski does not explicitly teach converting data into block data for encryption. Wasilewski teaches encrypting the data with the DES protocol (Col 9 lines 8-12), Daemen teaches using a predetermined block size of 128bits (page 8 "Specification). Thus Wasilewski teaches that the MPEG stream must be converted into 128 bit blocks to be encrypted. Wasilewski teaches outputting encrypted stream data, thus the 128 bit blocks are converted from blocks back into bytes (Col 9 lines 30-36). Wasilewski does not teach buffers.

It would be obvious one of ordinary skill in the art to use the apparatus of Wasilewski with the protocol of Daemen to provide an encryption scheme that is efficient for use with low-end microprocessors.

Mroczkowski teaches data inputted from the control unit and then stores corresponding result in the output buffer of the control unit (Mroczkowski, section 2.1).
It would be obvious one of ordinary skill in the art to use the apparatus of Wasilewski with the protocol of Mroczkowski to provide an encryption scheme that is efficient for use with low-end microprocessors. .

As per clams 3, and 13 Wasilewski does not specify completeing all round calculations and storing the result in a corresponding output buffer. Mroczkowski teaches implementing a block cipher wherein a block round unit (Mroczkowski, Figures 1 and 2) completes all round calculation of data having been currently encrypted or decrypted before a next block data (Mroczkowski, input data) inputted from the control unit and then stores corresponding result in the output buffer of the control unit (Mroczkowski, section 2.1).
It would be obvious one of ordinary skill in the art to use the apparatus of Wasilewski with the protocol of Mroczkowski to provide an encryption scheme that is efficient for use with low-end microprocessors.

Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski US 5,420,866 in view of Daemen ("AES Proposal: Rijndael," March 1999), in view of Vanstone US 6,212,281.

As per claims 25-27, Wasilewski teaches a control unit receiving a data stream of byte units where the data stream is an MPEG data stream (encoder) (Col 8 lines 52-60, Col 9 lines 58). Daemen teaches that a cipher key (start signal) is sent upon which the round keys are derived.on page (4.3). Daemen teaches using an input to generate a key according to schedule and size (expansion). Daemen teaches a key size (page 14 4.3) and an expansion algorithm for the Rijndael block cipher wherein the key expansion unit expands the inputted key value (page 14, section 4.3.1). It is inherent that the cryptographic process happens in real time when it is initiated by key expansion input. It would be obvious one of ordinary skill in the art to use the apparatus of Wasilewski with the protocol of Daemen to provide an encryption scheme that is efficient for use with low-end microprocessors.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER J. BROWN whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571)272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher J Brown/ 6/9/08
Primary Examiner, Art Unit 2439